Для цитирования: Молчанов И. А., Пузырев Д. В., Гусев М. В. Реализация системы криптографической защиты информации вычислительного комплекса // Вопросы радиоэлектроники. 2017. № 3. С. 76–82.
УДК 004.056.53:004.3

И. А. Молчанов[1,2], Д. В. Пузырев[3], М. В. Гусев[1,2]

[1] АО «МЦСТ», [2] ПАО «ИНЭУМ имени И. С. Брука», [3] ООО «Фирма АНКАД»

РЕАЛИЗАЦИЯ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА

В статье сформулированы задачи системы криптографической защиты информации в составе вычислительного комплекса (ВК). Рассмотрены основные классы несанкционированного доступа по виду нарушаемого свойства информации и сформулированы типы изделий, осуществляющих защиту от данных угроз. На основе этого анализа проведен выбор конкретных классов систем, подлежащих включению в состав ВК, к которому предъявляются требования Федеральной службы по техническому и экспортному контролю (ФСТЭК) России к защищенности информации от несанкционированного доступа.

Ключевые слова: *криптографическая защита информации, вычислительные комплексы семейства Эльбрус, защита от несанкционированного доступа, доверенная загрузка, аппаратное шифрование, удаленное управление.*

Введение

В настоящее время к системам, обрабатывающим конфиденциальную информацию, а также информацию, отнесенную к государственной или коммерческой тайне, предъявляются достаточно жесткие требования. Хотя для ликвидации типичных угроз, характерных для автоматизированных систем (АС) обработки информации, комплексы предпринимаемых согласно этим требованиям мер совершенно необходимы, тем не менее в том случае, когда меры не соответствуют угрозам, возможны недопустимые последствия [1]. Недооценка угрозы приводит к утечке или подмене защищаемой информации, а переоценка – к неоправданным затратам при эксплуатации АС, как прямым (финансовые и временные затраты на проверки, сертификацию и т.д.), так и косвенным (неудобства для персонала и, как следствие, пониженная эффективность работы, ошибочные действия, а также намеренное игнорирование мер защиты) [2, 3]. По этим причинам в зависимости от назначения АС система защиты информации, как правило, создается на основе определенной модели угроз.

Тем не менее в общем случае АС состоит из определенных модулей, многие из которых разрабатываются не исключительно для нее, а значит, должны удовлетворять различным моделям угроз. Это может обеспечиваться либо завышением требований, предъявляемых к модулям, либо гибким приведением конфигурации к вариантам, предусмотренным для моделей предполагаемых угроз. Применительно к средствам вычислительной техники оба данных подхода применимы и оправданы.

В данной статье описаны группы требований к защищенности компонентов ВК, предназначенного для применения в АС различных классов, и приведен пример реализации в нем системы криптографической защиты информации с возможностью удаленного управления.

Защита информации в вычислительных комплексах

В рассматриваемом случае под защитой информации понимается предотвращение несанкционированного доступа, который нарушает правила разграничения доступа и осуществляется с использованием штатных средств, предоставляемых вычислительным комплексом или автоматизированной системой в целом [4], и его последствий.

В терминологии средств защиты угрозы делятся на три основных класса по виду нарушаемого свойства информации: 1) конфиденциальности; 2) целостности; 3) доступности. При этом во многих случаях наиболее серьезными считаются угрозы первых двух типов. Следовательно, в ВК, к которым предъявляются требования к защищенности информации, необходимо предусмотреть использование тех средств, которые реализуют защиту от нарушения всех трех приведенных свойств либо первых двух, поскольку в большинстве АС их нарушение считается более опасным.

Для защиты от нарушения конфиденциальности информации, т.е. ее утечки, перехвата, съема, копирования, хищения или разглашения, применяются средства криптографической защиты информации (СКЗИ), которые могут представлять собой аппаратные, аппаратно-программные и программные изделия. Для защиты от нарушения целостности информации применяются методы, позволяющие определить факт модификации информации, например, электронная подпись. Кроме того, исключить угрозы первых двух типов позволяют меры разграничения доступа, разрешающие запись и/или чтение информации только правильно идентифицированным и аутентифицированным пользователям. В качестве подобных систем применяются средства парольной и ключевой защиты (с помощью программных и аппаратных средств, в т.ч. носителей ключевой информации), а также программные и аппаратно-программные модули доверенной загрузки (ПМДЗ и АПМДЗ) [5].

В данной статье под средствами криптографической защиты будут пониматься прежде всего:

- средства доверенной загрузки обоих типов;
- аппаратные и программные шифраторы (абонентские, канальные, шифраторы накопителей);
- ключевые носители, используемые для аутентификации и загрузки ключей в перечисленные средства;
- служебное программное обеспечение (ПО) ВК или АС в целом, служащее целям защиты информации от несанкционированного доступа.

Поскольку ключевые носители и ПО являются служебными средствами и сами по себе не реализуют криптографической защиты, детально в работе будут рассмотрены аппаратные средства доверенной загрузки и аппаратные шифраторы.

Доверенная загрузка

Доверенная загрузка операционной системы (ОС) может обеспечиваться с помощью программных («МДЗ-Эшелон», Altell Trust) и аппаратно-программных (АПМДЗ «Центурион», «Максим-М1», «Соболь», «КРИПТОН-АПМДЗ») модулей. В статье будут рассмотрены аппаратно-программные модули доверенной загрузки (АПМДЗ), пригодные для построения вычислительных средств, используемых в АС, защищенных от несанкционированного доступа в соответствии с требованиями ФСТЭК и ФСБ России.

При рассмотрении данного вопроса важно помнить, что сам принцип использования модуля доверенной загрузки как средства защиты работает только в том случае, если есть возможность ограничить физический доступ злоумышленника к вычислительному устройству. В противном случае извлечь модуль и тем самым нарушить безопасность будет вполне возможно. Но, несмотря на такое жесткое ограничение, модули доверенной загрузки являются важным звеном в обеспечении безопасности информационной системы.

В обязательные функции модуля входят:

- аутентификация пользователя до запуска основной ОС;
- протоколирование событий безопасности;
- контроль целостности программной и аппаратной платформ;
- доверенная загрузка ОС.

Под доверенной загрузкой ОС подразумевается, что модуль должен гарантировать загрузку именно той ОС, с которой разрешено работать конкретному пользователю. Например, пользователю обычно запрещено загружаться со сменных носителей.

ВК обладает обширной поверхностью атаки. В общем объеме исполняемого на нем программного кода существуют уязвимости, возможны даже закладки. Поэтому разработка АПМДЗ и связанных систем безопасности ведется на основании многоуровневой модели:

1. Микроконтроллер модуля – самый безопасный уровень. Это физически отдельная микросхема с ограниченной функциональностью, соединенная с внешним миром ограниченным числом интерфейсов, поэтому защитить ее намного проще, чем остальные компоненты.
2. Уровень программы начального старта (в т.ч. BIOS), на котором работает оболочка модуля. Он достаточно безопасен, т.к. первым получает управление, и до него (а тем более параллельно с ним) не исполняется потенциально опасный код. Тем не менее он уязвим, т.к. использует общие ресурсы (память, процессор, устройства и т.д.), взаимодействует с большим количеством интерфейсов и, как следствие, имеет значительную поверхность атаки.
3. Уровень, на котором могут находиться код системного управления, гипервизор системы аппаратной виртуализации или другой. Он исполняется параллельно с потенциально опасным кодом, но отделен механизмами процессора (SMI, VT-x и т.д.) и находится в отдельном диапазоне адресов, что позволяет связать с ним некоторую степень надежности.
4. Уровень ядра ОС – это драйверы, системные сервисы и другие составляющие. Этот уровень отделен от следующего кольцами защиты.
5. И, наконец, уровень приложений, которые защищаются друг от друга изоляцией процессов ОС с использованием страничной адресации памяти.

Чем сильнее безопасность системы зависит от функции, тем на более защищенном уровне она должна исполняться. Например, аутентификация пользователя, как локальная, так и сетевая, работа с перманентными секретами (ключи аутентификации и шифрования), авторизация доступа к ресурсам АПМДЗ, криптографическая защита канала при централизованном администрировании, протоколирование событий безопасности и некоторые другие функции выполняются в микроконтроллере. Контроль целостности и доверенная загрузка ОС выполняются в оболочке, работающей на стадии программы начального старта.

Так как программные методы лишены самого защищенного уровня, то они не подходят для высоких классов защиты. Это ограничивает их применение автоматизированными системами низких классов защиты, в то же время в АС высоких классов защиты используются исключительно аппаратно-программные методы. Кроме того, АПМДЗ часто используются в качестве корня доверия (root of trust), который может реализовать множество дополнительных функций:

- тракт ввода ключей для СКЗИ;
- функциональность Trusted Platform Module (TPM) [6];
- централизованное распространение ключей, обновление микропрограмм шифраторов и других СКЗИ;
- доверенную загрузку дополнительных средств защиты, таких как гипервизор и терминальный клиент;
- управление внешними устройствами: магнитной защелкой корпуса, подключением/отключением устройств в зависимости от прав пользователя, устройствами обеспечения многоконтурности защиты и др.

Шифрование

Среди шифрующих устройств следует выделить три основных класса, каждый из которых включает как аппаратные (и аппаратно-программные), так и чисто программные средства:

1. Абонентские шифраторы, позволяющие зашифровывать и расшифровывать блоки данных по командам пользователя.
2. Канальные шифраторы, дающие возможность производить прозрачную для пользователя криптозащиту данных, передаваемых по каналам связи.
3. Шифраторы накопителей для прозрачной по отношению к пользователю криптозащиты данных, размещенных на устройствах хранения.

Далее будут рассмотрены аппаратные средства шифрования, пригодные для построения ВК, используемых в АС высоких классов защиты от несанкционированного доступа (2А, 1Б, 1А в соответствии с требованиями ФСТЭК России).

Как программные, так и аппаратные средства шифрования реализуют математическое преобразование информации. Различия между ними можно разделить на три группы, соответствующие эксплуатационным и юридическим аспектам, а также характеристикам безопасности.

Очевидные эксплуатационные преимущества программных средств – это низкая стоимость владения и простота эксплуатации, а недостатки – малая производительность в силу недостаточной загрузки процессора. Юридические требования для информации, составляющей государственную тайну и имеющей гриф «совершенно секретно» (или выше), делают почти обязательным использование аппаратных шифраторов. В этом случае программное шифрование хоть и допустимо, но является редким исключением, т.к. обеспечить выполнение криптографических и инженерно-криптографических требований в программе, работающей на автоматизированном рабочем месте (АРМ) очень сложно, поэтому здесь главным образом используются аппаратные шифраторы.

Основная сложность аппаратного шифрования – это удовлетворение требований по вероятности ошибки зашифровывания, вероятности компрометации криптографически опасной информации, и особенно – требований к побочному электромагнитному излучению и наводкам (ПЭМИН).

С точки зрения безопасности программные шифраторы принципиально уязвимы для атак со стороны другого ПО, т.к. ключи шифрования и другая криптографически опасная информация, а также программный код шифратора находятся в разделяемой памяти компьютера. В аппаратном шифраторе, как правило, ключи никогда не появляются в разделяемой памяти, а реализация практически неуязвима для программных воздействий.

В контексте данного раздела существенна устойчивость аппаратного шифрования к любому программному коду, который может быть исполнен злоумышленником на защищаемом компьютере, – компьютерным вирусам, закладкам, намеренно эксплуатируемым ошибкам функционирования штатного ПО.

Основная угроза, от которой защищает проходной шифратор диска (ПШД), – это хищение информации, расположенной на накопителе. Если программа-нарушитель получит доступ к ключам шифрования, то появится возможность, например, сохранить их на тот же диск в открытом виде. Очевидно, что в случае аппаратного шифрования

это невозможно, т.к. диск шифруется независимо от программного окружения.

Шифраторы накопителей на твердотельных элементах памяти («флэш-дисках») дополнительно могут обеспечивать доступ к диску только на чтение или только на запись, взаимную аутентификацию дисков и шифратора, ведение журнала и другие функции безопасности, программная реализация которых была бы настолько же уязвима для программы-нарушителя, как и шифрование.

Проходной интерфейсный (как правило, сетевой) шифратор защищает от кражи или подмены данных в соответствующем канале связи. Уязвимости программного шифратора аналогичны предыдущему случаю, т.е. программа-нарушитель может послать в сеть ключи или информацию в открытом виде. Кроме того, существует особенность с точки зрения защиты от косвенных каналов утечки. Любая программа, в т.ч. шифратор, использует разделяемые ресурсы – процессор, память, жесткий диск. Поэтому программа-нарушитель может, например, модулируя загрузку ресурсов компьютера, легко воздействовать на скорость приема/передачи трафика, т.е. организовать косвенный канал утечки, даже если у нее нет привилегий для непосредственного воздействия на средства защиты. В то же время аппаратные шифраторы могут обеспечивать статистическую неразличимость трафика вне зависимости от того, что происходит в ПО АРМ.

Возможность применения абонентских шифраторов ограничена прежде всего тем, что с заданной вероятностью ошибки тяжело доказать, была ли использована зашифрованная, а не открытая информация. С другой стороны, их применение гарантирует выполнение требований по компрометации ключей и другой криптографически опасной информации, по вероятностям ошибки зашифровывания, по побочным электромагнитным излучениям и наводкам, а кроме того – формальных требований по использованию аппаратных шифраторов в АС, обрабатывающих информацию, которая составляет государственную тайну. Их часто используют для организации дополнительных контуров шифрования, в аппаратуре децентрализованного изготовления ключей, в специализированных АРМ, для которых легко обеспечить замкнутость программной среды, и т.д.

Удаленное управление

Одним из важных требований к вычислительным средствам, применяемым в больших количествах в АС, является возможность удаленного управления. Как правило, используются двухуровневая («контроллер уровня блока (Shelf/Chassis Manager) – контроллер уровня платы (Baseboard Management Controller) – материнская плата») или одноуровневая («контроллер удаленного управления – материнская плата») схема. Двухуровневая схема предназначена прежде всего для модульных устройств, устанавливаемых в стандартный субблок (например, форм-факторов CompactPCI, VPX, VME, AdvancedTCA), одноуровневая – для монолитных блоков, собираемых в стойку.

В качестве таких контроллеров применяются, как правило, аппаратные решения в виде микросхем (Avago Pilot 3, ASPEED AST 2400) и модулей (Pentair ChMM-700R, R500S_MNGR). Основными требованиями к таким модулям и микросхемам являются поддержка протокола управления Intelligent Platform Management Interface (IPMI), возможность управления по Ethernet («IPMI over LAN») с использованием протокола Remote Management Control Protocol (RMCP), отслеживание системных датчиков (температура, скорость вращения вентиляторов, напряжения), удаленная индикация устройства (Unit ID), прямое подключение к текстовому или графическому терминалу вычислительного устройства («KVM over IP»), резервируемость и «горячая замена», независимость от работоспособности основной системы, приоритет управления по IPMI над локальным управлением из ОС и т.п. В ситуации защищенного ВК дополнительно к перечисленному выдвигается требование невозможности несанкционированного управления. Обеспечивать такую функциональность можно с помощью криптографически защищенных (в т.ч. и с использованием аппаратных шифраторов) каналов между модулем удаленного управления и АРМ администратора безопасности.

Реализация защищенного вычислительного комплекса

В качестве защищенного ВК, удовлетворяющего предъявляемым требованиям, можно отметить ВК «Эльбрус-804», разработанный ПАО «ИНЭУМ им. И.С. Брука». Он построен на базе разработанных АО «МЦСТ» микропроцессоров «Эльбрус-8С» и контроллера периферийных интерфейсов («южного моста») КПИ-2 с использованием базового технического решения для многопроцессорных ВК семейства «Эльбрус» [7]. Данный комплекс работает под управлением ОС «Эльбрус», основанной на дистрибутиве Debian ОС GNU/Linux, и поддерживает широкий набор ПО, включая как общее, так и специальное ПО, предназначенное для организации АС соответствующего назначения.

ВК «Эльбрус-804», функциональная схема которого приведена на рисунке, обладает следующими характеристиками:

- тип микропроцессоров – «Эльбрус-8С» (1891ВМ10Я);
- количество микропроцессоров – 4;

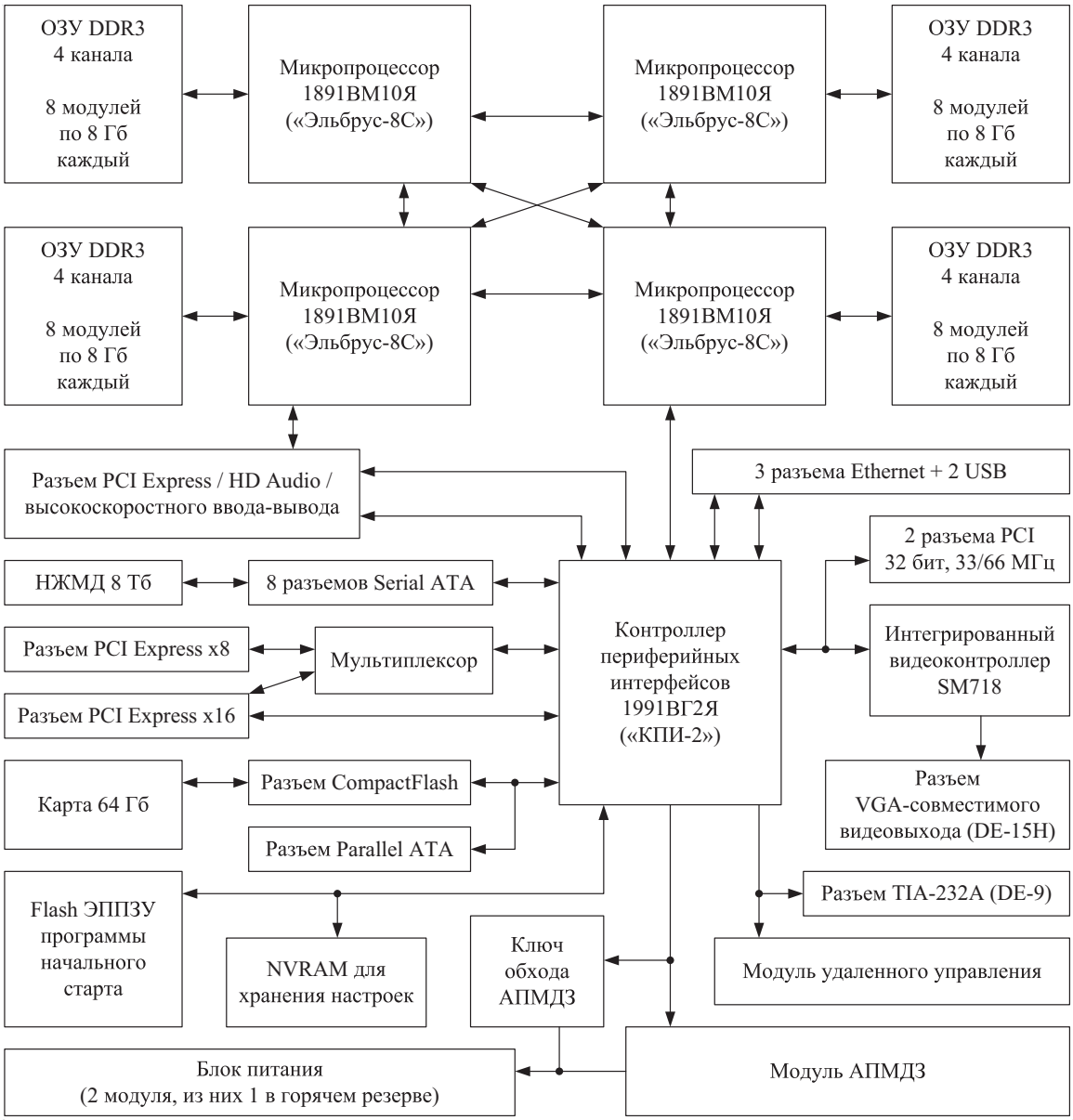

Рисунок. Функциональная схема ВК «Эльбрус-804»

- тактовая частота процессора – от 600 до 1300 МГц, номинальная – 900 или 1200 МГц в зависимости от исполнения;
- оперативная память – в базовой комплектации 256 Гб DDR3 (по 64 Гб на процессор);
- накопители данных – в базовой комплектации 8 Тб на жестком диске форм-фактора 3,5", а также карта CompactFlash объемом 64 Гб для нужд бинарного транслятора кода архитектуры IA-32 (x86);
- интегрированная периферия: 1 канал TIA-232A (RS-232), 1 VGA-совместимый видеовыход, 3 канала Ethernet 802.3ab, 6 каналов USB2.0; доступно 7 из 8 разъемов Serial ATA, 1 разъем Parallel ATA, 2 слота PCI 32 бита, 33/66 МГц, 3 слота PCI Express в конфигурации x4+x16 или x4+x8+x8; в слот x4 может быть установлена также специализированная карта скоростного ввода-вывода или карта аудиокодека, совместимая с SupremeFX фирмы ASUS;
- конструктивное исполнение: стоечный корпус с возможностью одностороннего обслуживания размерами 3U×19"×450 мм;
- питание: от сети переменного тока 220 В, 50 Гц, резервирование блока питания типа «1+1», выходная пиковая мощность блока питания до 1000 Вт, средняя потребляемая мощность при полной нагрузке 700 Вт;
- система охлаждения: принудительная воздушная, проточная, холодный коридор с передней стороны.

Система защиты информации (СЗИ) данного комплекса построена на основе аппаратно-про-

граммного модуля доверенной загрузки «Макет АПМДЗ-ЗУС» (И/Э) разработки ООО «Фирма АНКАД». СЗИ выполнена с учетом требований ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ класса 1А или 1Б, а ВК, включающий данный модуль, – с учетом требований ФСТЭК России [8], предъявляемым к СВТ 2-го класса защищенности от несанкционированного доступа. Проводятся работы по получению соответствующих сертификатов.

При необходимости комплекс может быть оснащен модернизированными сетевыми шифраторами серии КРИПТОН-AncNet и/или модернизированными проходными шифраторами диска серии КРИПТОН-ПШД. Это позволит использовать его при построении АС, удовлетворяющих классам 2А, 1Б, 1А защиты от несанкционированного доступа в соответствии с требованиями ФСТЭК России [9].

Кроме того, данный комплекс может поставляться без аппаратных и аппаратно-программных СКЗИ для использования в областях, где не требуется обработка конфиденциальной информации или информации, составляющей государственную, коммерческую или иную тайну. Такая возможность позволяет унифицировать вычислительную технику, применяемую в различных контурах защиты АС, и использовать ее в качестве базовой в следующих случаях:

- в контурах, где не требуется защита информации, – ВК без СКЗИ;
- в контурах, где требуется защита информации от несанкционированного доступа, удовлетворяющая требованиям ФСТЭК к АС классов 3Б, 3А, 2Б, 1Д, 1Г, 1В, – ВК с АПМДЗ, но без прочих СКЗИ;
- в контурах, где требуется защита информации от несанкционированного доступа, удовлетворяющая требованиям ФСТЭК к АС классов 2А, 1Б, 1А, – ВК с АПМДЗ и прочими СКЗИ.

Система удаленного управления комплексом реализована на основе отдельно поставляемого модуля, устанавливаемого заказчиком в соответствующий разъем на системной плате ВК. В этом качестве можно использовать модули ShMM-700R, PPMM-700R производства фирмы Pentair, а также модуль R500S_MNGR производства АО «МЦСТ». Возможна также защита канала связи, в т.ч. и с использованием аппаратных шифраторов, устанавливаемых в систему.

Комплекс снабжен пятидюймовым стандартным отсеком накопителя, в который возможна установка заказчиком блока экстренного гарантированного уничтожения информации с магнитных или полупроводниковых (твердотельных) носителей, например, «Импульс-SSD» или «Импульс-6В Mini» разработки ООО «Детектор Системс». С помощью этого устройства можно избежать компрометации информации при попытке несанкционированного изъятия носителя или угрозы такой попытки путем необратимого уничтожения информации.

Заключение

Поскольку ВК семейства «Эльбрус» построены на основе разработанных в России электронных компонентов, они используются в таких областях, где важно отсутствие закладок в аппаратуре, обрабатывающей информацию, составляющую государственную, коммерческую или другие виды тайны. Система защиты от несанкционированного доступа, реализация которой рассмотрена в данной статье, дополнительно позволит строить на их основе, и, в частности, на основе ВК «Эльбрус-804», автоматизированные системы высоких классов защищенности, что может способствовать повышенному спросу со стороны заинтересованных организаций.

СПИСОК ЛИТЕРАТУРЫ

1. Ставер Е.В. Защита информации в автоматизированных системах обработки информации // Международн. науч. конференция «Информационные технологии и системы 2012» (ИТС 2012): Сб. докл. Минск, БГУИР, 2012. С. 246–247.
2. Амелин Р.В. Информационная безопасность [Электронный ресурс]. URL: http://nto.immpu.sgu.ru/system/files/3/__77037.pdf (дата обращения: 02.11.2016).
3. Торопцев Е.Л., Репин А.В. Информационная безопасность и стандарт CobiT // Молодой ученый. 2014. № 8. С. 112–115.
4. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения: Решение председателя Гостехкомиссии России от 30 марта 1992 г.
5. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности. 2016. № 1 (14). С. 24–30.
6. TPM Library Specification. Trusted Computing Group [Электронный ресурс]. URL: http://www.trustedcomputinggroup.org/tpm-library-specification/ (дата обращения: 22.11.2016)
7. Бычков И.Н., Молчанов И.А., Рябцев Ю.С. Развитие конструкций многопроцессорных систем // Вопросы радиоэлектроники. 2016. № 3. С. 22–29.
8. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Решение председателя Гостехкомиссии России от 30 марта 1992 г.

9. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Решение председателя Гостехкомиссии России от 30 марта 1992 г.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Молчанов Игорь Анатольевич, инженер, АО «МЦСТ», ПАО «ИНЭУМ им. И.С. Брука», 119334, Москва, ул. Вавилова, д.24, тел.: 8 (499) 135-62-02, e-mail: igor.a.molchanov@mcst.ru.
Пузырев Дмитрий Вячеславович, начальник отдела, ООО «Фирма АНКАД», 124527, Зеленоград, Солнечная аллея, д.8, тел.: 8 (909) 976-85-96, e-mail: puzirev@ancud.ru.
Гусев Максим Викторович, инженер, АО «МЦСТ», ПАО «ИНЭУМ им. И.С. Брука», 119334, Москва, ул. Вавилова, д.24, тел.: 8 (499) 135-62-02, e-mail: maksim.v.gusev@mcst.ru.

For citation: Molchanov I.A., Puzyrev D.V., Gusev M.V. Implementation of cryptographic protection for a complex computing system. Voprosy radioelektroniki, 2017, no. 3, pp. 76–82.

I.A. Molchanov, D.V. Puzyrev, M.V. Gusev

IMPLEMENTATION OF CRYPTOGRAPHIC PROTECTION FOR A COMPLEX COMPUTING SYSTEM

Tasks of system that implements a cryptographic protection of sensitive information in a computing system are discussed in this paper. Types of unauthorized access classified by violated property of information are listed. Analysis of device types implementing counteractions to these violations is performed. Based on this analysis, classes of devices that should be included in a computing system which complains to Federal Service for Technical and Export Control of Russia regulations for unauthorized access prevention are determined.

Keywords: cryptographic protection, Elbrus computing systems, unauthorized access prevention, trusted boot, hardware-based encryption, platform management.

REFERENCES

1. Staver E.V. Information protection in automated information processing systems. *Mezhdunarodn. nauchn. konferentsiya «Informatsionnye tekhnologii i sistemy 2012» (ITS2012). Sb. dokl.* Minsk, BGUIR, 2012, pp. 246–247 (In Russian).
2. Amelin R.V. [Information security] (In Russ.). Available at: http://nto.immpu.sgu.ru/system/files/3/__77037.pdf (accessed: 02.11.2016)
3. Toroptsev E.L., Repin A.V. Information security and CobiT standard. *Molodoi uchenyi.* 2014, no. 8, pp. 112–115 (In Russian).
4. Rukovodyashchii dokument. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya [Unauthorized access prevention. Terms and conditions]. Reshenie predsedatelya Gostekhkomissii Rossii ot 30 marta 1992 g. (In Russian).
5. Avezova Y.E., Fadin A.A. Problems of trusted boot implementation for physical and virtualized environments. *Voprosy kiberbezopasnosti,* no. 1 (14), 2016, pp. 24–30 (In Russian).
6. [TPM Library Specification. Trusted Computing Group] (In Russ.). Available at: http://www.trustedcomputinggroup.org/tpm-library-specification/ (accessed: 22.11.2016)
7. Bychkov I.N., Molchanov I.A., Ryabtsev Yu.S. Evolution of multiprocessor system constructions. *Voprosy radioelektroniki,* 2008, no. 3, pp. 22–29 (In Russian).
8. Rukovodyashchii dokument. Sredstva vychislitelnoi tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [Computing devices. Unauthorized access prevention. Properties of unauthorized access withstanding]. Reshenie predsedatelya Gostekhkomissii Rossii ot 30 marta 1992 g. (In Russian).
9. Rukovodyashchii dokument. Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii [Automated systems. Unathorized access prevention. Automated systems classification and requirements to information protection]. Reshenie predsedatelya Gostekhkomissii Rossii ot 30 marta 1992 g. (In Russian).

AUTHORS

Molchanov Igor, engineer, JSC «MCST», PJSC «Brook INEUM», 24, Vavilova st., Moscow, 119334, Russian Federation, tel.: +7 (499) 135-62-02, e-mail: igor.a.molchanov@mcst.ru.
Puzyrev Dmitriy, lead programmer, ANCUD LLC, 8, Solnechnaya all., Zelenograd, 124527, Russian Federation, tel.: +7 (909) 976-85-96, e-mail: puzirev@ancud.ru.
Gusev Maksim, engineer, JSC «MCST», PJSC «Brook INEUM», 24, Vavilova st., Moscow, 119334, Russian Federation, tel.: +7 (499) 135-62-02, e-mail: maksim.v.gusev@mcst.ru.